

What is claimed is:

1. A method for implementing a risk management program, comprising:
establishing one or more checklist items that measure risk factors and one or more
procedures for determining compliance with the checklist items;

wherein trusted parties perform an assessment of each of the entities based on the checklist items using the procedures and, based on the assessment, perform at least one of the following: (i) dispense a machine-readable trust assertion comprising one or more attributes relating to a result of the assessment and (ii) revoke a previously-issued machine-readable trust assertion comprising one or more attributes relating to a result of a previously-performed assessment.

2. The method of claim 1 further comprising:
establishing one or more context factors used in performing the assessment, wherein the context factors comprise at least one of an entity identifier and an entity organizational structure.
3. The method of claim 1 wherein the result of the assessment comprises a trust assertion score associated with the checklist items.
4. The method of claim 2 wherein the result of the assessment comprises a scope of the assessment, determined based on the context factors, wherein the scope of the assessment comprises an identifier for the assessed entity, a portion of the entity included in the assessment, and any portion of the entity excluded from the assessment.
5. The method of claim 1 wherein the checklist items comprise industry-specific checklist items.
6. The method of claim 1 wherein the procedures comprise industry-specific procedures.
7. The method of claim 1, further comprising:
certifying the trusted parties in accordance with a certification process established by a consortium, wherein the consortium performs an assessment of the trusted parties based on the certification process, and, based on the assessment, performs at least one of (i) dispenses a machine-readable trust assertion comprising one or more attributes relating to a result of the assessment and (ii) revokes a previously-issued machine-readable trust assertion comprising one or more attributes relating to a result of a previously-performed assessment.

8. The method of claim 1, wherein the risk factors relate to one or more of security, safety, supply chain, and finances.
9. The method of claim 1 wherein the trust assertion comprises a digital certificate.
10. The method of claim 1 wherein the checklist items are established by a consortium.
11. The method of claim 2 wherein the context factors are established by a consortium.
12. A method for conveying an assessment of an entity, comprising:
 - receiving from an entity a machine-readable trust assertion issued by a trusted party resulting from an assessment of the entity,
 - wherein the assessment is based on one or more checklist items that measure risk factors and one or more procedures for determining compliance with the checklist items;
 - analyzing the trust assertion to determine (1) an identity of the trusted party, (2) checklist items used in the assessment, (3) a score of the assessment, (4) a scope of the assessment; and (5) a date of the assessment;
 - comparing the identity of the trusted party, the checklist items used in the assessment, the score, the scope and the date to an acceptable trusted party identity, acceptable checklist items, an acceptable score, an acceptable scope and an acceptable date; and
 - determining, based on the comparison, trustworthiness of the entity.
13. The method of claim 12 wherein the trust assertion comprises a digital certificate comprising one or more attributes relating to the trust assertion.
14. The method of claim 13 further comprising:
 - analyzing the digital certificate to determine validity.
15. The method of claim 14, wherein the validity determination comprises determining if the digital certificate has been revoked.
16. The method of claim 12, further comprising:
 - analyzing the trust assertion to determine integrity.
17. The method of claim 14, wherein analyzing the digital certificate comprises analyzing cryptographic components in the digital certificate.
18. The method of claim 12 wherein the identity of the trusted party is embodied in a digital certificate, signed by a consortium asserting that the trusted party is viable and certified by the consortium.
19. The method of claim 18 further comprising:

analyzing the digital certificate of the trusted party to determine if the digital certificate has been revoked.

20. The method of claim 12 wherein the trust assertion score is represented in binary format.

21. The method of claim 20 wherein the trust assertion score is provided in a hexadecimal representation of the binary format.

22. The method of claim 12 wherein the trust assertion score is provided as a sum of binary scores, in base-10 numeral format.

23. The method of claim 12 wherein a consortium establishes one or more context factors used in performing the assessment, wherein the context factors comprise at least one of an entity identifier and an entity organizational structure, and wherein the scope of the assessment is determined based on the context factors and comprises an identifier for the assessed entity, a portion of the entity included in the assessment, and any portion of the entity excluded from the assessment.

24. The method of claim 12 wherein the trust assertion score is represented for at least one of the checklist items to have not been assessed.

25. The method of claim 12 further comprising:
analyzing formatted data associated with the trust assertion.

26. The method of claim 12 wherein the checklist items that measure risk factors and the procedures are established by a consortium.

27. A method for implementing trust governance for an entity, comprising:
generating one or more templates relating to trustworthiness requirements for the entity, based on at least one of an entity policy, any exceptions to the policy and any rules restricting or enabling variances to the policy; and a contractual obligation of the entity;
receiving one or more trust assertions in connection with a trust relationship between two or more entities, wherein the trust assertions are issued by a trusted party resulting from an assessment of one of the entities and comprise components of making a trust decision, comprising one or more of an identity of the trusted party; one or more checklist items that measure risk factors used in the assessment; a score of the assessment; a scope of the assessment; and a date of the assessment;

identifying one or more of the templates to apply to the trust assertion;

comparing the trust assertion to the identified templates; and

determining a result based on the comparison, the result comprising at least one of an acceptance, a rejection and a processing status message.

28. The method of claim 27 wherein the templates are machine-readable.

29. The method of claim 27 wherein the trust assertions are machine-readable.

30. The method of claim 27, further comprising:

performing one or more actions, indicated in the one or more identified templates, associated with at least one of the result and attributes of the assessment.

31. The method of claim 27 wherein one or more of the templates facilitates conversion of a trust assertion of a first type to a trust assertion of a second type.

32. The method of claim 27 wherein the trust relationship relates to one or more transactions.

33. The method of claim 32 wherein the components of making the trust decision further comprise an identity of the transaction.

34. The method of claim 33 wherein the components of making the trust decision further comprise a date of the transaction.

35. The method of claim 27, wherein each of the templates comprise one or more of a portion of the entity covered by the template, and any portion of the entity excluded by the template; checklist items that measure risk factors used by the portion of the entity covered by the template; a score required by the template; an issuer of the template; an issue date of the template; and an expiry date of the template.

36. The method of claim 27, wherein the trust assertion is compared to the identified templates in a specified order.

37. The method of claim 27, wherein the trustworthiness requirements relate to one or more of security, safety, supply chain, and finances.

38. The method of claim 27 wherein the components of making the trust assertion further comprise a date of the determining step.

39. A method for modeling trust relationships, comprising:

collecting one or more trust assertions for an entity, relating to a trust relationship between the entity and one or more other entities, wherein each of the trust assertions is issued by a trusted party resulting from a risk factor assessment of the entity and comprises components of making a trust decision, comprising one or more of an identity of the trusted party; checklist

items that measure risk factors used in the assessment; a score of the assessment; a scope of the assessment; and a date of the assessment;

storing the trust assertions;

generating one or more templates relating to trustworthiness requirements for the entity, based on at least one of an entity policy, any exceptions to the policy and any rules restricting or enabling variances to the policy; and a contractual obligation of the entity;

storing the templates;

effectuating a change in at least one of the templates or generating one or more new templates; and

based on a comparison of the stored trust assertions to one or more of (i) the stored templates and (ii) the new templates, determining the impact of the change or the new template on the trust relationship.

40. The method of claim 39 wherein the templates are machine-readable.

41. The method of claim 39 wherein the trust relationship relates to one or more transactions.

42. The method of claim 39, further comprising:

collecting one or more of the trust assertions for one of the other entities; and
storing the trust assertions of the other entity;

wherein determining the impact of the change or the new template on the trust relationship is further based on a comparison of the stored templates to the stored trust assertions of the other entity.

43. The method of claim 41 wherein the components of making the trust decision further comprise an identity of the transaction.

44. The method of claim 43 wherein the components of making the trust decision further comprise a date of the transaction.

45. The method of claim 39 wherein one or more of the templates facilitates conversion of a trust assertion of a first type to a trust assertion of a second type.

46. A method for modeling trust relationships comprising:

collecting one or more trust assertions for one entity relating to a trust relationship with another entity;

storing the trust assertions of the one entity; and

analyzing the trust assertions of the one entity to determine how the trust assertions have changed over time.

47. A method for modeling trust relationships comprising:

collecting one or more trust assertions for at least two first entities relating to a trust relationship with a second entity;

storing the trust assertions of the at least two first entities; and

comparing the trust assertions of at least one of the first entities to at least one other of the first entities.